Staking Architecture v2

Stake DAO

May 2025

Disclaimer: This white paper is provided for information purposes only and does not constitute financial, legal, or investment advice, nor is it a solicitation or offer to buy or sell any financial instrument or participate in any investment activity in any jurisdiction. Participation in Vaults v2 protocol involves risks, including, but not limited to, market volatility, technical vulnerabilities, and regulatory uncertainty. Users are solely responsible for ensuring that their use of the protocol complies with all laws and regulations applicable to them, including those relating to anti-money laundering (AML), counter-terrorism financing (CTF), and economic sanctions. Users must not use the protocol if they are located in, incorporated in, or otherwise subject to the laws of any jurisdiction where such use would be prohibited. Past or simulated performance (including APY figures) is not indicative of future results and should not be relied upon as a guarantee of returns. All figures presented herein are for illustrative purposes only. StakeDAO Association does not guarantee the functionality or security of the Staking Architecture v2 protocol, despite having undergone independent security audits. This white paper and the Staking Architecture v2 protocol do not currently implement Know Your Customer (KYC) procedures, but this may change in the future in response to evolving legal and regulatory requirements. The Staking Architecture v2 smart contracts are licensed under the Business Source License (BSL), and use or copying of any portion of the code prior to the expiration or public release date without prior written consent from the StakeDAO Association is strictly prohibited and may result in legal action. Users are advised to consult independent legal and financial professionals before interacting with the protocol.

1 Introduction

The year 2020 marked the emergence of yield aggregators[1] in Decentralized Finance (DeFi). These protocols offer user-friendly, gas-efficient, and boosted access to yield generation in DeFi. All of these protocols (including Stake DAO, Yearn, Convex, Beefy, etc.) operate on the same general principle: pooling of user funds, rewards harvesting, and distribution.

Although most of these protocols disappeared after the DeFi summer, those that remain still work on the same infrastructure. However, this architecture has significant limitations that reduce the value proposition of yield aggregators.

Vaults v2[2] brings a significant update to the traditional yield aggregator architecture that aims to solve those issues and improve the user experience.

[1] Participants should be aware of the risks associated with decentralized finance, including but not limited to smart contract vulnerabilities, market risks, and regulatory uncertainties. Staking Architecture v2 is subject to potential hacking, fraud, and other malicious activities that could result in partial or total loss of funds.

[2] The term "Vault" refers to a "non-custodial vault contract". For clarity, terms such as 'strategy', 'vault', and 'boost' refer to automated smart contract behaviors and do not imply discretionary management, investment services, or custodial activity.

2 Understanding the current yield aggregation architecture

As previously mentioned, all yield aggregators operate on the principle of pooling funds and rewards. Let's look at Stake DAO's current architecture. To benefit from Stake DAO's boost on a certain protocol (let's take Curve as an example) by depositing into a Stake DAO strategy[3], a user will first need to deposit into the corresponding vault, a gas efficient contract that accumulates funds before sending them to the gas-heavy strategy. Then funds are transferred to the strategy, after which they are transferred to the locker, and finally deposited inside the Curve gauge. To be eligible for rewards, the user then needs to stake its liquidity provision token (LP token) into the Stake DAO Gauge, a smart contract in charge of distributing the rewards generated by the strategy.

Once this is done, rewards will start accumulating on Curve. When there are enough rewards, they are harvested (claimed) by the protocol in a decentralized way, and sent to the Stake DAO Gauge for distribution. This distribution is performed by the Gauge contract. Rewards are accrued based on contract logic over a seven-day period to users, proportionately to their share of the total LP tokens staked in the gauge. The reason for streaming the rewards is to prevent bad actors from gaming the harvests and only staking right before the harvest and unstaking right after, while not generating any reward by staying during the whole period in the strategy.

[3]The term "strategy" refers solely to predefined smart contract logic used to interact with DeFi protocols. Nor Stake DAO, neither Staking Architecture v2 do not offer discretionary asset management or personalized financial advice. Users self-select strategies and interact with smart contracts at their own initiative.

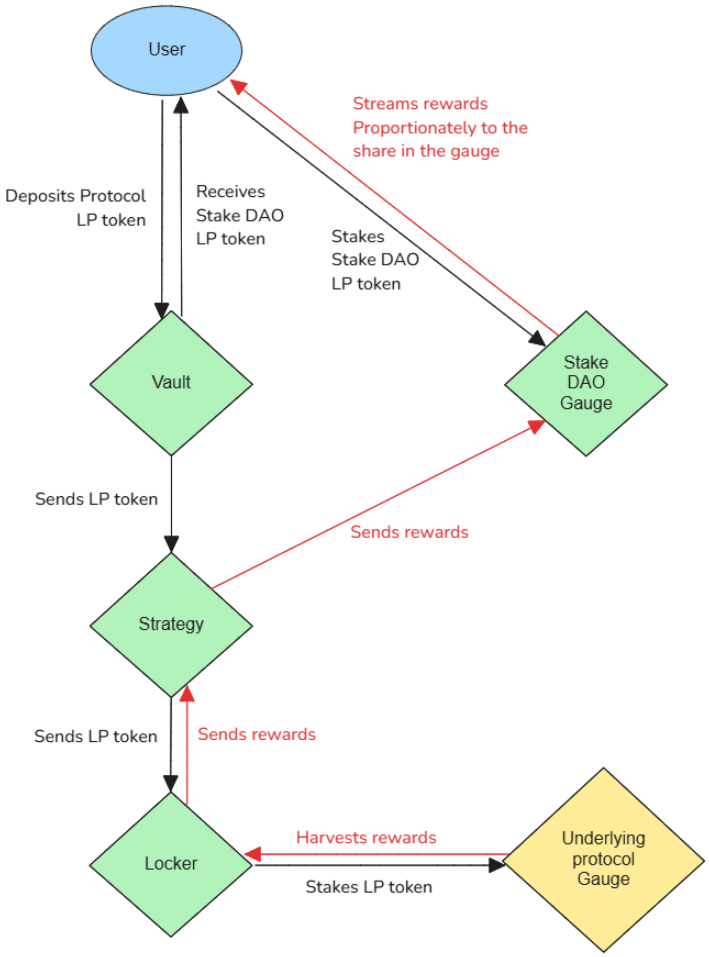

Figure 1: Stake DAO's current staking infrastructure

2.1 The limitations of the existing model[4]

The current infrastructure has several limitations that reduce its value proposition. It works well for users whose deposits represent a small fraction of the vault's total value locked (TVL). However, large deposits relative to the vault's TVL create dilution effects that negatively impact user returns.

Let us take an example, assuming that funds are harvested weekly, and ignoring boost and fees for simplicity. While funds are typically harvested more frequently in practice, this does not change the fundamental dynamics.

In the following example, there is a pool with a TVL of $700, none of which is going through a yield aggregator. This pool receives $10 of rewards every week. At the end of Week 1, Bob deposits $300 through a yield aggregator.

During Week 2, the Aggregator accumulates $3 of harvestable rewards. At the end of Week 2, these rewards are harvested and start streaming over seven days to Bob, who therefore receives those $3 of rewards during Week 3, while the aggregator

[4]The APYs shown are theoretical examples based on historical data or simulations. Actual performance may vary and is not guaranteed.

accumulates another $3 of harvestable rewards.

At the end of Week 3, Alice deposits $400 in the pool through the aggregator. The total pool TVL is now $1,400 while the aggregator has a TVL of $700.

During Week 4, the aggregator therefore accumulates $5 of rewards, while the $3 of Week 3 rewards (generated by Bob's funds) are distributed to Bob and Alice proportionately to their share in the aggregator's TVL. Bob receives $1.29 and Alice $1.71.

During Week 5, the aggregator accumulates another $5 of rewards and streams Week 4 rewards to Bob and Alice, who respectively receive $2.14 and $2.86. At the end of Week 5, Alice withdraws her funds from the pool.

During Week 6, Bob receives the $5 of rewards from Week 5 (partially accumulated by Alice's funds), while the aggregator accumulates $3 of harvestable rewards that will be distributed to Bob during Week 7.

	TVL				Rewards			
	Pool	Aggregator	Bob	Alice	Pool	Aggregator	Bob	Alice
Week 1	700	-	-	-	10.00	-	-	-
Week 2	1,000	300	300	-	10.00	3.00	-	-
Week 3	1,000	300	300	-	10.00	3.00	3.00	-
Week 4	1,400	700	300	400	10.00	5.00	1.29	1.71
Week 5	1,400	700	300	400	10.00	5.00	2.14	2.86
Week 6	1,000	300	300	-	10.00	3.00	5.00	-
Week 7	1,000	300	300	-	10.00	3.00	3.00	-
Total					70.00	22.00	14.43	4.57
APY							51.3%	34.6%

Table 1: TVL & Rewards distribution with current yield aggregator architecture

In this example, Bob achieves a 51.3% APY and Alice achieves a 34.6% APY. But what else did we witness?

- There is a one-week delay between Bob's deposit and his first rewards. Similarly, Alice's rewards only reach its run-rate amount after one week.
- After Alice deposits, Bob's rewards decrease for one week. That is because Alice's funds have not generated rewards yet and she is effectively squatting Bob's rewards.
- When Alice withdraws her funds from the pool, she forfeits one week of rewards ($2.86). Those rewards are given instead to Bob.
- If the pool failed to be harvested for one week, Bob and Alice would not receive any rewards for this week, and would risk those rewards being squatted after the next harvest.

Now let us take a look at what this would look like if rewards were instantly distributed to Bob and Alice by the aggregator.

	TVL				Rewards claimable immediately			
	Pool	Aggregator	Bob	Alice	Pool	Aggregator	Bob	Alice
Week 1	700	-	-	-	10.00	-	-	-
Week 2	1,000	300	300	-	10.00	3.00	3.00	-
Week 3	1,000	300	300	-	10.00	3.00	3.00	-
Week 4	1,400	700	300	400	10.00	5.00	2.14	2.86
Week 5	1,400	700	300	400	10.00	5.00	2.14	2.86
Week 6	1,000	300	300	-	10.00	3.00	3.00	-
Week 7	1,000	300	300	-	10.00	3.00	3.00	-
Total					70.00	22.00	16.29	5.71
APY							59.9%	44.9%

Table 2: TVL & Rewards distribution if users could claim their rewards immediately

We see that with rewards immediately claimable, Bob and Alice's APY gain broadly 10 points. It is a 16% increase in APY for Bob and a 30% increase in APY for Alice. There is definitely room for improvement in the current yield aggregator architecture, and this is what this new architecture is aiming for.

3 Staking Architecture v2: a new reward distribution mechanism for accelerated user return[5]

3.1 General architecture

Staking Architecture v2 addresses current limitations by delivering rewards to users instantly and accurately. This is made possible because, although user funds are still pooled together in a contract, rewards are no longer mutualized. An Accountant contract manages individual reward allocations, updating each user's claimable balance with every interaction, making sure every user always receives exactly the amount of rewards that their funds generated. Since this Accountant contract knows exactly what rewards are given to whom, there is no more risk of users taking advantage of harvests or strategy price increase by doing sandwich deposits and withdraw, or a similar kind of behavior. This means that it is no longer necessary to stream rewards collected by the strategy, and those rewards can therefore be distributed instantly to users, giving the user the same experience as if they were depositing directly on the underlying protocol.

[5]All material changes to the protocol — including fee structures, smart contract upgrades, and protocol shutdowns — are subject to governance proposals and on-chain voting by token holders or DAO-designated voters.

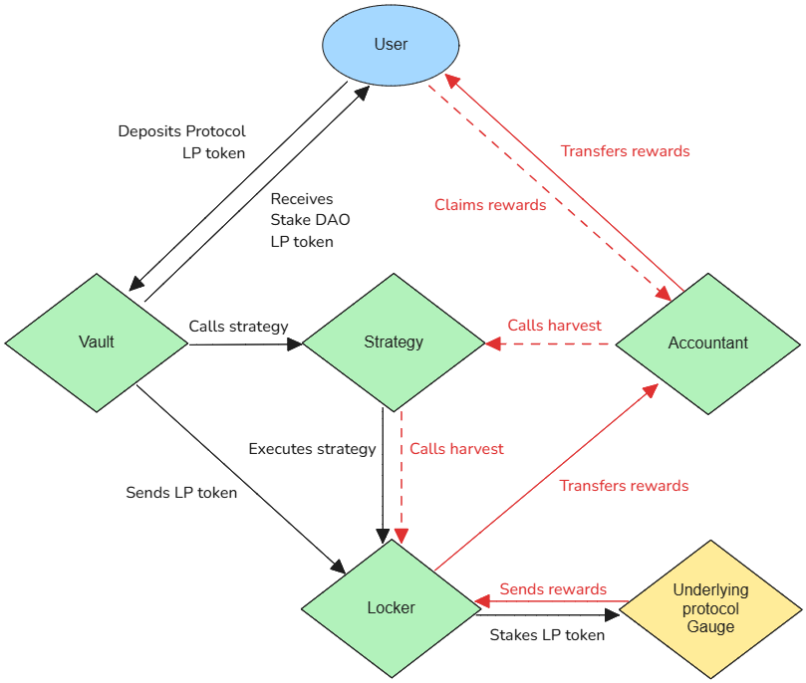

Figure 2: Staking Architecture v2

3.2 Cross-vault reward pooling

In the current architecture, the rewards harvested from one pool are distributed to depositors of the corresponding vault. For instance, if a user deposits in a Stake DAO strategy that has not been harvested for more than seven days, they will need to wait for someone to harvest the corresponding pool before starting to receive any reward. Harvests typically occur when it is profitable for the harvester to do so, and hence when there is enough claimable rewards so that the harvester fee covers the gas cost of claiming plus a little profit. In the case of new pools, or pools that are not receiving a lot of rewards, or simply have a low TVL, it can be complicated to have weekly harvests.

Each DeFi protocol distributes a primary reward token (e.g., CRV for Curve, PENDLE for Pendle, dYFI for Yearn, BAL for Balancer, etc.). While in the current architecture it is necessary to silo the rewards for accounting purposes (otherwise it would not be possible to distribute rewards properly), the Accountant contract of this new architecture knows exactly how much is claimable by each address, so there is no need to treat rewards separately anymore. Therefore, in Vaults v2, there is one Accountant contract per underlying protocol, and rewards from all pools are pooled together in the Accountant contract. When depositing funds in a Vault v2, users immediately see their claimable rewards ramping up, and can claim whenever they want. When they claim, their rewards do not have to come from the pool where their funds are staked. They pull those rewards from the Accountant contract which receives all the rewards from all the harvests for this underlying protocol.

This significantly reduces harvest costs. With its current harvest incentivization mechanism (0.5% fee on rewards harvested), Stake DAO has strategies that are harvested every five minutes while others rarely are. With reward pooling, the harvester fee can be lowered significantly. Initially, harvester fee will be set at 0.05% ,

but will be a variable that can be adjusted by Stake DAO's decentralised governance to reach the optimal figure minimising the harvester fee for the user while keeping the desired user experience. Any change in the fee design and adjustment rules will be subject to a vote in Stake DAO's governance.

3.3 Management of extra-rewards

Extra rewards are pool-specific and cannot be aggregated like primary rewards. These will continue using the traditional distribution mechanism.

3.4 Summarizing Staking Architecture v2 benefits

Thanks to this new way of managing rewards and harvests, Vaults v2 offer several key improvements over traditional yield aggregators:

1. **Instant reward distribution:** the seven-day delay between the moment the user's funds generate the rewards and the moment the user receives them does not exist anymore;
2. **Full reward portability:** upon withdrawal, users can claim all accrued rewards generated by their funds;
3. **No reward dilution:** the Accountant contract prevents new depositors from diluting existing users' rewards;
4. **No pause of rewards if the pool is not harvested:** thanks to reward pooling, users can always claim the rewards they generate;
5. **Reduced harvest costs:** initial harvester fees are 90% lower than current rates (0.05% vs 0.5%)..

Furthermore, Staking Architecture v2 will also be compatible with OnlyBoost, making them the most attractive solution for liquidity provision on all supported protocols.

These improvements enable dynamic fund management across all Stake DAO vaults. Since no rewards are lost by leaving a vault to join a new one, and since the yield does not take seven days to ramp up anymore, it is now possible to optimally manage funds by jumping from one vault to the other, to always chase the best yield possible.

This opens the door to curated strategies built on top of Vaults v2: professional actors will be able to have their own strategy where anyone can deposit, and that they will manage optimally, with settings they define.[6]

4 Security and compliance

4.1 Permission system

The protocol implements a granular permission system through ProtocolController:

- Function-level permissions for contract interactions;

[6] Users agree to comply with the terms of service and all applicable laws. Any use of Vaults v2 for illicit activities including, but not limited to, money laundering, terrorist financing, or fraud is strictly prohibited and will result in immediate suspension and reporting to relevant authorities.

- Designated permission setters for managing access;
- Owner-controlled critical functions.

4.2 Emergency shutdown

Two levels of emergency shutdown are available:

1. Gauge shutdown:
    - Disables operations for a specific gauge
    - Allows users to withdraw funds
2. Protocol shutdown:
    - Disables all operations for a protocol integration
    - Affects all gauges associated with the protocol

The Staking Architecture v2 will be protected by Hypernative, which will be able to activate those emergency shutdown options in case a potential attack is detected.

4.3 Audits

Staking Architecture v2 contracts have been audited by Trust Security and Omniscia.

Audit reports are available in Stake DAO's documentation. Though these audits increase security, users should understand that no system can guarantee complete protection against risks or vulnerabilities.

Moreover, while the Staking Architecture v2 has undergone audits by reputable firms, smart contracts are inherently subject to risk. Exploits, bugs, or vulnerabilities may still exist. Users should exercise caution and only deposit funds they are prepared to lose. Past audits do not guarantee future security.

4.4 Compliance and security warning

We encourage all users to perform their own due diligence before using Vaults v2. Blockchain technology and DeFi platforms are experimental and carry inherent risks, including potential loss of funds or rewards. Users participate at their own discretion and risk.

Users are also encouraged to stay informed of any regulatory changes that may affect their participation. Stake DAO does not guarantee compliance with every jurisdiction's laws, and advises users to consult local regulations and legal advisors

Stake DAO does not guarantee compliance with every jurisdiction's laws, and advises users to consult local regulations and legal advisors. Neither the StakeDAO Association nor its contributors assume responsibility for any direct, indirect, or consequential losses resulting from the use of this protocol.

Additionally, Staking Architecture v2 does not issue or sell tokens as financial instruments. If a token is used in connection with the protocol (e.g., for governance or staking), it may not represent any legal claim, share, or entitlement to income or assets of any kind. The token should not be considered an investment.

4.5 Regulatory status

Staking Architecture v2 is a decentralized financial infrastructure operating without centralized intermediaries. As such, it does not hold user assets or client funds in custody. The StakeDAO Association acts solely as a technical contributor and governance facilitator.

The protocol has not been registered or authorized as a financial service provider in any jurisdiction. Users are responsible for verifying their own legal eligibility to interact with decentralized finance systems in their country of residence.

4.6 Fee governance and transparency

All protocol fees, including but not limited to harvest fees, boost rental fees, and protocol fees, are transparently defined in the smart contracts and associated documentation. The initial harvester fee is set at 0.05%, significantly lower than the previous model's 0.5%. Any changes to the protocol-configured incentives will be subject to DAO governance proposals and on-chain voting. Users are encouraged to consult the Stake DAO governance portal for real-time fee updates and proposal discussions.

5 Intellectual property

Staking Architecture v2's code and smart contracts are open-source and licensed under the Business Source License (BSL). This license protects the code until the earlier of January 1, 2028, or a date specified at stakingv2-license-date.stakedao.eth. Before this date, any party intending to fork or copy all or parts of Staking Architecture v2's code or contracts must obtain prior permission from StakeDAO Association. Interested parties should contact us via contact@stakedao.org to discuss the terms and conditions for potential use.[7][8]

[7] All code and smart contracts are released under the Business Source License (BSL), ensuring transparency and collaborative improvements. Unauthorized use of the code before the specified date will be pursued legally to the fullest extent.

[8] This document and any related agreements shall be governed by and construed in accordance with the laws of Switzerland. All disputes arising out of or in connection with this document shall be resolved through arbitration under the Swiss Arbitration Centre. The seat of arbitration shall be in Zug, Switzerland, and the proceedings shall be conducted in English. The arbitration shall be final and binding on the parties involved.